УДК 004.56:61

д.т.н., проф. **Лукова-Чуйко Н.В.** (КНУ)
д.т.н., проф. **Толюпа С.В.** (КНУ)
к.є.н, доц. **Погасій С.С.** (ХНЕУ)
Лаптєва Т.О. (КНУ)
Лаптєв С.О. (КНУ)

DOI: https://doi.org/10.17721/2519-481X/2021/73-10

УДОСКОНАЛЕННЯ МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

В Україні право на приватність – це конституційна гарантія, а захист персональних даних – одна із сфер, у якій така гарантія має реалізовуватись. Предметом нашого дослідження будуть не об'єкти взагалі, а динамічні системи захисту інформації в соціальних мережах у математичному розумінні цього терміну. Описи динамічних систем для різноманітних задач в залежності від закону еволюції різноманітні: за допомогою диференціальних рівнянь, дискретних відображень, теорії графів, теорії марківських ланцюгів тощо. Вибір одного із способів опису задає конкретний вигляд математичної моделі відповідної динамічної системи. Теоретичне дослідження динамічної поведінки реального об'єкта вимагає створення його математичної моделі. Більшість відомих підходів до моделювання, відрізняються тім, які параметри при моделюванні ними використовують в якості вхідної інформації та які характеристики модельованої системи розраховуються та надходять на вихід моделі. В роботі дослідження моделей захисту інформації. Продовжуються розробка математичної моделі захисту інформації в соціальної мережі в залежності від специфічних її параметрів. Модель удосконалюється за рахунок врахування специфіки соціальних мереж. Таких як: довіра, репутація, вплив загроз безпеки даних від розповсюдження інформації між користувачами, вплив загроз безпеки даних від взаємовпливів користувачів, вплив загроз безпеки даних від взаємодії користувачів та вплив загроз безпеки даних від довжини шляху між користувачами. Однак слід означити, що параметрів соціальної мережи значно більше. Але ці параметри ми вважаємо найбільш впливовими. Тому приділяємо увагу саме на цих специфічних параметрах.

Проведено математичне моделювання удосконаленої моделі захисту інформації у соціальної мережі в залежності від специфічних її параметрів. При моделювання введені обмеження та припущення які дозволили отримати графічні результати. Графічні результати відображають актуальну картину захисту інформації соціальної мережи від зовнішніх впливів. Отримані результати підтверджують адекватність розробленої математичної моделі захисту інформації у соціальної сеті.

Ключові слова: соціальна мережа, довіра, репутація, моделювання, коефіцієнт захисту, безпека, захист інформації

Вступ та постановка задачі. Виходячи з реалій сьогодення ефективність функціонування будь-якої організації, підприємства та держави залежить не тільки від надійності функціонування інформаційно - телекомунікаційних систем, а й у значній мірі від захищеності їх інформаційних ресурсів та інформації взагалі.

Предметом нашого дослідження будуть не об'єкти взагалі, а динамічні системи захисту інформації в соціальних мережах у математичному розумінні цього терміну.

Описи динамічних систем для різноманітних задач в залежності від закону еволюції різноманітні: за допомогою диференціальних рівнянь, дискретних відображень, теорії графів, теорії марківських ланцюгів тощо. Вибір одного із способів опису задає конкретний вигляд математичної моделі відповідної динамічної системи [1 - 4]. Теоретичне дослідження динамічної поведінки реального об'єкта вимагає створення його математичної моделі. У багатьох випадках процедура розробки моделі полягає в складанні математичних рівнянь на основі фізичних законів. Зазвичай ці закони формулюються на мові диференціальних рівнянь. В результаті координати стану системи і її параметри виявляються пов'язаними між собою, що дозволяє приступити до вирішення диференціальних рівнянь при різних початкових

умовах і параметрах. Тому розробка нових та удосконалених методів підвищення рівня захищеності інформаційного простору соціальних мереж, які базуються на математичних моделях динамічних систем є дуже актуальною.

Аналіз останніх досліджень. Більшість відомих підходів до моделювання, відрізняються тім, які параметри при моделюванні ними використовують в якості вхідної інформації та які характеристики модельованої системи розраховуються та надходять на вихід моделі (будують моделі з Використання теорії ймовірностей, випадкових процесів, мереж Петрі, теорії автоматів, теорії графів, нечітких множини, теорії катастроф, ентропійного підходу та ін.).

При цьому аналітичні моделі, що розглядаються з позиції теоретичної математики не тотожні реальної дійсності, зважаючи на обмежену точність результатів. [1,3].

У [2,4] розглядається модель інформаційної безпеки на основі Марковських випадкових процесів. Отримані чисельні значення, однак вони розглядають питання загрози уразливості. Питання загроз уразливості не торкається питання взаємозалежності основних параметрів моделі, що можливо призводить до ускладнення моделювання процесу.

У [5] звертається увага на нестійкість і отже, великі варіації отриманих рішень при поганій обумовленості систем лінійних алгебраїчних рівнянь і неточно заданих значень ефектів і результатів спостережень. Це пов’язане з питанням не врахування взаємозалежності основних параметрів

Разом з тим у всіх зазначених джерелах математичне моделювання розглядається як математична модель конкретних параметрів (деякі параметри мають імовірнісний характер) Питання взаємозв'язку вхідних параметрів при моделюванні процесів глибину їх взаємозв'язку моделі не розглядають. Ці чинники взаємозв'язку і взаємовпливу можуть істотно спотворити результати моделювання і поставити під сумнів адекватність моделі.

В роботах [6,11] досліджуються моделі окремих складових специфічних параметрів мережі. В роботі [7] розглянуто метод розрахунку захисту інформації від репутації користувачів при нелінійній залежності параметрів. В статях [8,12] досліджуються загальні параметри безпеки в мережах. В роботах [9] вказуються ризики безпеки в соціальних мережах. В статях [10,15] розглядається захист в соціальних мережах від небажаної інформації. В роботі [16] розглядається захист персональної інформації користувачів. В статті [17] - метод розрахунку захисту інформації від взаємовпливу користувачів в соціальних мережах.

Разом з тим у всіх зазначених джерелах математичне моделювання розглядається як математична модель конкретних параметрів (деякі параметри мають імовірнісний характер) Питання взаємозв'язку вхідних параметрів при моделюванні процесів глибину їх взаємозв'язку моделі не розглядають. Ці чинники взаємозв'язку і взаємовпливу можуть істотно спотворити результати моделювання і поставити під сумнів адекватність моделі

Таким чином, на даний час в практиці і теорії побудови та експлуатації соціальних мереж існує об’єктивне протиріччя між необхідністю підвищення рівня захищеності інформації в соціальних мережах та недосконалістю системи захисту інформації соціальних та можливостями існуючих методів, які використовуються системою захисту інформації в соціальних мережах. Тому розробка та удосконалення математичних моделей захисту інформації у соціальних мережах є актуальним завданням.

Метою роботи є удосконалення моделі захисту даних у соціальної мережи за рахунок врахування специфіки соціальних мереж. Таких як: довіра, репутація, вплив загроз безпеки даних від розповсюдження інформації між користувачами, вплив загроз безпеки даних від взаємовпливів користувачів, вплив загроз безпеки даних від взаємодії користувачів та вплив загроз безпеки даних від довжини шляху між користувачами.

Виклад основного матеріалу. Математична модель динамічної системи вважається заданою, якщо введені параметри (координати) системи, що визначають однозначно її стан, і зазначений закон еволюції. Залежно від ступеня наближення одній і тій самій системі можуть бути поставлені у відповідність різні математичні моделі.

Теоретичне дослідження динамічної поведінки реального об'єкта вимагає створення його математичної моделі. У багатьох випадках процедура розробки моделі полягає в складанні математичних рівнянь на основі фізичних законів. Зазвичай ці закони формулюються на мові диференціальних рівнянь. В результаті координати стану системи і її параметри виявляються пов'язаними між собою, що дозволяє приступити до вирішення диференціальних рівнянь при різних початкових умовах і параметрах.

У класичному підході до захисту даних розрізняють:

$$T_i = \left[D_j, D_n, D_m, D_k \right], \tag{1}$$

де T_i – множина загроз від втрати довіри між користувачами;

D_j – довіра на надання послуг, людина довіряє стороні в наданні якісних послуг провайдером послуг або ресурсів;

D_n – довіра делегування (delegation trust) описує довіру в користувача (представника), що діє і виносить рішення від імені сторони, якій довіряє;

D_m – довіра доступу (access trust) описує довіру довіряє зі сторони (провайдера) до користувача, яким надається доступ до ресурсів. Це – контроль доступу. Використовується в системах автентифікації;

D_k – контекстна довіра визначає міру віри учасника в необхідні системи та інституційні механізми, що підтримують транзакції і забезпечують безпеку мережі.

Втрата такої якості, як довіра – процес, який має часовий інтервал [4,11]. Позначимо кількість інформації в системі – I. Потік інформації за межі інформаційної системи через *dI*–, швидкість зміни цього потоку – $\frac{dI}{dt}$. Логічне, що якщо потік і швидкість зміни потоку дорівнюють нулю, то витоку інформації немає:

$$dI = 0; \frac{dI}{dt} = 0 \quad . \tag{2}$$

Витік інформації залежить від захищеності системи – вжитих заходів з нейтралізації загроз безпеки даних. Z – показник захищеності інформаційної системи. Загалом витік інформації залежить:

- від розміру інформаційної системи (отже, в якійсь мірі і від кількості даних);
- від швидкості витоку даних
- витік інформації купірується захищеністю системи (заходами щодо нейтралізації загроз безпеки інформації).

Тоді з урахуванням введених позначень, отримуємо рівняння для швидкості витоку інформації:

$$\frac{dI}{dt} = Z_p Z + (C_v + C_k) I \quad , \tag{3}$$

де Z_p – коефіцієнт, що відображає вплив заходів щодо захисту інформації;

Cv – коефіцієнт, що відображає вплив швидкості витоку даних;

C_k – коефіцієнт, що відображає вплив кількості даних на їх витік.

Для подальшого виведення моделі захисту інформації будемо розглядати захищеність системи (Z). Для цього визначимо захищеність системи як здатність системи протистояти несанкціонованому доступу до конфіденційної даних. Отже, захищеність системи буде залежати:

- від розмірів системи (як і від кількості даних);
- загроз безпеки інформації від втрати довіри між користувачами.

Тоді з урахуванням введених позначень, отримуємо рівняння для можливості швидкого захисту інформації від витоку:

$$\frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) \ , \tag{4}$$

де D_i – коефіцієнт, що відображає вплив загроз безпеки даних від втрати довіри між користувачами на захищеність інформаційної системи.

C_{d2} – коефіцієнт, що відображає вплив розмірів системи на захищеність;

C_{d1} – коефіцієнт, що відображає вплив захищеності на витік даних.

Тоді отримуємо систему рівнянь. Яка складається з рівнянь (3) і (4):

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) \end{cases} . \tag{5}$$

Але система рівнянь (5) є базовою системою, має лінійних характер. Це відповідає процесу захисту інформації у де яких випадках. Які більш носять стаціонарні вже вивчені процеси впливу на захист інформації.

Тому головною відмінністю нашої моделі на першому етапі, е модель яка відрізняється наявністю «малого параметру». Тобто для рішення потрібно використовуватися спеціальні методи. Малий параметр у нашому випадку буде змінюватися по випадковому закону. Це обумовлено відсутністю чітко визначених законів витоку або пошкодження інформації. Система рівнянь прийме вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + \varepsilon(C_v + C_K) I \\ \frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1})\varepsilon \end{cases} , \tag{6}$$

Знайдемо стаціонарну позицію системи, що описується рівняннями (6). Умови стаціонарності $dI = 0; \frac{dI}{dt} = 0$. Отже:

$$\begin{cases} Z_p \bar{Z} + \varepsilon(C_v + C_K) \bar{I} = 0 \\ D_i - I(C_{d2} + Cd_1)\varepsilon = 0 \end{cases} . \tag{7}$$

З другого рівняння системи слідує:

$$\bar{I} = \frac{D_i}{(C_{d2} + C_{d1})\varepsilon} \ . \tag{8}$$

Далі з першого рівняння системи рівнянь (6) знаходимо $\bar{Z}$.

$$Z_p \bar{Z} - \frac{(C_v + C_K) D_i}{(C_{d2} + C_{d1})\varepsilon} = 0 \ , \tag{9}$$

$$\bar{Z} = \frac{(C_v + C_K) D_i)}{(C_{d2} + C_{d1})\varepsilon Z_p} \ . \tag{10}$$

Результати обрахунків за рівнянням (9)

Отже, умови позиції стаціонарності системи:

$$\begin{cases} \bar{I} = \dfrac{D_i}{(C_{d2} + Z_p)\varepsilon} \\ \bar{Z} = \dfrac{(C_v + C_K)D_i}{(C_{d2} + C_{d1})\varepsilon Z_p} \end{cases}. \quad (11)$$

Вирішимо систему рівнянь (6) методом «малих відхилень»

$I = \bar{I} + I; Z = \bar{Z} + Z$:, отже, система рівнянь прийме вигляд:

$$\begin{cases} \dfrac{dI}{dt} = Z_p(\bar{Z} + Z) + (C_v + C_K)(\bar{I} + I) \\ \dfrac{dZ}{dt} = D_i - (\bar{I} + I)(C_{d2} + C_{d1})\varepsilon \end{cases}, \quad (12)$$

$$\begin{cases} \dfrac{dI}{dt} = (C_{d1} + C_{d2})\varepsilon Z - (C_v + C_K)I \\ \dfrac{dZ}{dt} = -I(C_{d2} + C_k) + D_i) \end{cases}. \quad (13)$$

Ця система диференціальних рівнянь е математичною моделлю захисту інформаціє у соціальної мережи від такого параметра, як довіра між користувачами.

Удосконалена математична модель системи захисту даних в соціальної мережи з урахуванням взаємовідносин користувачів

З метою розробки математичної моделі системи захисту даних в соціальній мережі з урахуванням взаємовідносин користувачів, введемо параметри взаємовідносин. Тоді математична модель буде представлена такою системою диференціальних рівнянь:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K)I \\ \dfrac{dZ}{dt} = (\alpha + \beta + \theta + \rho)V - I(C_{d2} + C_{d1})\varepsilon \end{cases}, \quad (14)$$

де V_i – коефіцієнт, що відображає вплив загроз безпеки даних від взаємодії між користувачами на захищеність інформаційної системи, параметр;

α - описує схильність суб'єкта до встановлення взаємодії;

β - описує привабливість або популярність;

θ – оцінка довіри;

ρ – характеристика тенденцій моделі до симетричності діад.

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K)I + L_2(I^2) + L_3(I^3) + \ldots \\ \dfrac{dZ}{dt} = (\alpha + \beta + \theta + \rho)V - I(C_{d2} + C_{d1}) + K_2(Z^2) + K_3(Z^3) + \ldots \end{cases}. \quad (15)$$

де L_2, L_3 і т.д. K_2, K_3 і т.д. деякі лінійні оператори. Будемо вважати не лінійність системи слабкою, що дозволяє шукати рішення для кожного рівняння системи (24) методом послідовного наближення, поклавши:

$$I = I_1 + I_2 + I_3 ...$$
$$Z = Z_1 + Z_2 + Z_3 + ...$$

Нехай при

$$dI = 0, \ \frac{dI}{dt} = 0, \text{ та } dZ = 0, \ \frac{dZ}{dt} = 0$$
$$I = I_0 \operatorname{Sin} \omega t, Z = Z_0 \operatorname{Sin} \omega t .$$

Отримаємо систему рівнянь:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I - L_2 (I_0{}^2 \operatorname{Sin}^2 \omega t) - L_3 (I_0{}^3 \operatorname{Sin}^3 \omega t) - ... \\ \frac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I (C_{d2} + C_{d1}) \varepsilon - K_2 (Z_0{}^2 \operatorname{Sin}^2 \omega t) - K_3 (Z_0{}^3 \operatorname{Sin}^3 \omega t) - ... \end{cases} . \quad (16)$$

Перепишемо систему і представимо її в такому вигляді:

$$\begin{cases} \frac{dI}{dt} = \alpha Z + \beta_1 I - \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t, \\ \frac{dZ}{dt} = \beta_2 \varepsilon I + \gamma - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} , \quad (17)$$

де $\alpha = Z_p$, $\beta_1 = C_v + C_K$, $\beta_2 = -(C_{d2} + C_{d1})$, $\gamma = (\alpha + \beta + \theta + \rho) V$

Система рівнянь (17) є математичною моделлю захисту інформації в у соціальної мережи з урахуванням такого специфічного параметра як взаємовідносини між користувачами. Слід зазначити, що у нашої моделі присутній «малий параметр». Малий параметр у нашому випадку буде змінюватися по випадковому закону. Це обумовлено відсутністю чітко визначених законів витоку або пошкодження інформації у залежності від взаємовідносин користувачів. Тобто для рішення потрібно використовуватися спеціальні методи. Тому будемо використаємо метод винятків:

$$\frac{dZ}{dt} = \beta_2 I + \gamma - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \Rightarrow I = \frac{1}{\beta_2} \left(\frac{dZ}{dt} - \gamma + \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \right) \Rightarrow$$

$$\frac{dI}{dt} = \frac{1}{\beta_2} \left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) \right) . \quad (18)$$

Підставимо всі найдені вирази в перше рівняння системи (6):

$$\frac{1}{\beta_2} \left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) \right) = \alpha Z + \frac{\beta_1}{\beta_2} \left(\frac{dZ}{dt} - \gamma + \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \right) -$$

$$- \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \ , \quad (19)$$

або:

$$\frac{d^2 Z}{dt^2} - \beta_1 \frac{dZ}{dt} - \alpha \beta_2 Z = - \frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) - \beta_1 \gamma + \beta_1 \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t -$$

$$-\beta_2 \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \,. \tag{20}$$

Тепер знаходимо спільне рішення відповідного однорідного рівняння:

$$Z'' - \beta_1 Z' - \alpha\beta_2 Z = 0 \,. \tag{21}$$

Характеристичне рівняння має вигляд: $\lambda^2 - \beta_1\lambda - \alpha\beta_2 = 0$. Розглянемо випадок позитивного дискримінанту цього рівняння:

$$D = \beta_1^2 + 4\alpha\beta_2 > 0 \Rightarrow \lambda_{1,2} = \frac{\beta_1 \pm \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} \,. \tag{22}$$

Звідкіля:

$Z_{одн}(t) = c_1 e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} + c_2 e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}$ - спільне рішення однорідного рівняння.

Для знаходження загального рішення неоднорідного рівняння скористаємося методом варіації довільних сталих: $Z_{одн}(t) = c_1(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} + c_2(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}$.

де $c_1'(t), c_2'(t)$ знаходяться із системи:

$$\begin{cases} c_1'(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} + c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} = 0, \\ c_1'(t)\dfrac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} + c_2'(t)\dfrac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} = N(t), \end{cases} \tag{23}$$

Остаточно:

$$\begin{aligned} Z(t) = \int N(t) - e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} \frac{e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}} dt - \\ - \int N(t) - e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} \frac{e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}} dt \end{aligned} \tag{24}$$

де

$$\begin{aligned} N = -\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_k Z_0^k \sin^{k-1}\omega t \cos\omega t\right) - \\ -\beta_1\gamma + \beta_1\sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t - \beta_2 \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \end{aligned} \,. \tag{25}$$

Система рівнянь (24) є математично моделлю системи захисту інформації з урахуванням такого специфічного параметра, як взаємовідносини між користувачами.

Вираз (25) є остаточним математичним результатом побудови цей моделі.

Удосконалення моделі захисту інформації за рахунок урахування взаємозв'язку користувачів

Для розробки моделі захисту інформації в залежності від взаємовпливу користувачів, необхідно доповнити систему рівнянь (23) параметром, який буде враховувати взаємодію між користувачами.

З цей метою візьмемо за основу Марьківську модель, яка найбільш адекватна для вирішення цього питання. Це обумовлено тім , що графічні моделі графів Маркова цілком

відповідають взаємозв'язку між користувачами. Взаємозв'язок між користувачами в цих моделях, цілком залежить від кількості користувачів. Які у свою чергу будуть являтися вершинами графа. Це цілком відповідає поставленому завданню, визначенню взаємозв'язків між користувачами. В зв'язку з тім, що Моделі Маркова достатньо вивчені, повносю модель описувати не будемо, обмежимось тільки визначенням коефіцієнту взаємозв'язку. Який буде визначатися наступним виразом:

$$Kv = (\frac{\sum_{v \in V} C_{v1}}{n^2}). \quad (26)$$

де $\sum_{v \in V} C_{v1}$ – загальна кількість з'єднань в мережі,

n –кількість вершин в мережі.

Тоді удосконалена модель прийме вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I(C_{d2} + C_{d1}) \varepsilon + (\frac{\sum_{v \in V} C_{v1}}{n^2}) \end{cases}. \quad (27)$$

Але специфіка соціальної мережи, специфічні параметри її потрібують більш ширшого розгляду. Наприклад соціальні мережи швидко розвіваються, але все ж таки мають обмеження. Це пов'язано з можливість мережи, зберігати та передавати дані. З цей метою будемо використовувати емпіричну модель. Особливістю застосування у нашому випадку буде те, що ми використовуємо епідемічну модель з ймовірністю передачі певної інформації, як функції відстані між джерелом і потенційною метою.

Тобто ймовірність, що m-й сусід передає цю інформацію особі, з яким він буде контактувати визначається як:

$$y = N_{knot}(r+1)^{-f} . \quad (28)$$

де: f>0 – ймовірна функція передачі інформації;

r –кількість користувачів з якими може поділитися даний користувач інформацією;

N_{knot} –користувач мережі, який знаходиться на визначеному вузлі.

З урахування вищевикладеного модель захисту параметрів у соціальної мережи прийме вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I(C_{d2} + C_{d1}) \varepsilon + \\ +(\frac{\sum_{v \in V} C_{v1}}{n^2}) + N_{knot}(r+1)^{-f} \end{cases}. \quad (29)$$

Удосконалення моделі захисту інформації за рахунок урахування центральності мережі

Метрики центральності – це кількісна оцінка тієї чи іншої особи в соціальній мережі. Міра центральності описує випуклість конкретного вузла в порівнянні з іншими вузлами. Середня міра центральності також відома як централізована оцінка, вона вказує, наскільки щільний граф по відношенню до кожного вузла. Центральні метрики, як правило, обчислюються на підставі всієї структури мережі або під графа.

Ступінь (рівень) центральності вузла (degree centrality) – це число зв'язків даного вузла з іншими вузлами. Використовувати такий вид центральності найкраще, коли необхідно

визначити людей, які вибирають Вас і з яким Ви віддаєте перевагу взаємодії [10] або, навпаки, від яких хочете триматися подалі. Формально ступінь центральності вузла можна представити в наступному вигляді :

$$C_D(i) = \sum_{j=1}^{n} a(i, j), \tag{30}$$

де CD (*i*) – степінь центральності вузла *i*;

a(*i*,*j*) – зв'язок між вершинами *i* та *j*,

n – число вершин в мережі; *a*(*i*,*j*) =1 тоді коли вершини з'єднані ребром.

Щоб можна було порівнювати степінь центральності вузла не тільки всередині одного графа, але і між графами різної структури [2], необхідно розрахувати нормовану центральність вузла, вона визначається виразом:

$$C_D(i) = \frac{C_D(i)}{n-1} \ . \tag{31}$$

де C'D (*i*) – нормована степінь центральності вузла *i*;

CD (*i*) – степінь центральності вузла і;

n – число вершин в мережі.

Величина C'D (i) змінюється в інтервалі від 0 до 1 і говорить про те, наскільки добре вершина і безпосередньо пов'язана з усіма іншими вершинами мережі. По суті, нормована степінь центральності вузла і є аналогом індексу соціометричного статусу члена групи (C_i), а нормована ступінь вихідної центральності вузла є аналогом індексу емоційної експансивності члена групи.

Щоб мати можливість порівняти різні структури і визначити, яка з них забезпечує найкращу централізацію вузлів, знаходять степінь центральності всього графа за формулою Фрімана [3]

$$C_D = \frac{\sum_{i=1}^{n} (C_D{}'(i) - C_D(i))}{(n-1)(n-2)} \ . \tag{32}$$

де C_D – степінь центральності всього графа;

$C_D{}'(i)$ – максимальний ступінь центральності вузла в мережі;

$C_D(i)$ – степінь центральності вузла і;

n – число вершин в мережі.

Тоді остаточне система диференціальних рівнянь математичної моделі захисту інформації з урахуванням центральності мережі прийме вид:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \dfrac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I(C_{d2} + C_{d1})\varepsilon + \\ +\left(\dfrac{\sum_{v \in V} C_{v1}}{n^2}\right) + N_{knot}(r+1)^{-f} + \dfrac{\sum_{i=1}^{n} (C_D{}'(i) - C_D(i))}{(n-1)(n-2)} \end{cases} . \tag{33}$$

Удосконалення моделі захисту інформації за рахунок урахування коефіцієнту довжени шляху інформації в соціальної мережі

З метою удосконалення моделі системи захисту соціальної мережі потрібно визначити, вплив коефіцієнта довжени шляху інформації на модель захисту інформації.

Для цього скористаємось моделлю Барабаш–Альберта. Середня довжина шляху в моделі Барабаш–Альберта збільшується в середньому, як логарифм розміру мережі. Точна форма має подвійну логарифмічну поправку і виглядає, як: $l \approx \frac{\ln n}{\ln \ln n}$.

Модель Барабаш–Альберта має систематично коротший середній шлях, ніж випадковий граф. Базуясь на цей моделі введемо коефіцієнт, якій враховує середню довжину шляху інформації у соціальної мережи: $\gamma = (\frac{\ln \ln n - n}{n(\ln \ln n)^2})$, де: n –кількість вершин в мережі.

Тоді математична модель прийме вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I(C_{d2} + C_{d1})\varepsilon + (\frac{\sum_{v \in V} C_{v1}}{n^2}) + \\ + N_{knot}(r+1)^{-f} + \frac{\sum_{i=1}^{n} (C_D^{'}(i) - C_D(i))}{(n-1)(n-2)} + (\frac{\ln \ln n - n}{n(\ln \ln n)^2}) \end{cases} . \quad (34)$$

Удосконалення моделі захисту інформації за рахунок урахування коефіцієнту взаємовпливу користувачів в соціальної мережі

З метою урахування взаємовпливу користувачів в соціальної мережі введемо коефіцієнт взаємовпливу:

$(P-N) \otimes (P+N)$ – коефіцієнт, що відображає вплив загроз безпеки інформації від взаємовпливу користувачів на захищеність інформаційної системи,

де P_{ij} –позитивний вплив між користувачами,

N_{ij} – негативний вплив між користувачами.

У цьому виразі ми використовуємо згортку двох функцій. Тому що взаємовплив не може бути визначено якимось цілим числом, тільки функцією. Це ще одно із головних відмінностей розробленої моделі. Система диференціальних рівнянь математичної моделі з урахуванням взаємовпливу користувачів прийме вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I(C_{d2} + C_{d1})\varepsilon + (\frac{\sum_{v \in V} C_{v1}}{n^2}) + \\ + N_{knot}(r+1)^{-f} + \frac{\sum_{i=1}^{n} (C_D^{'}(i) - C_D(i))}{(n-1)(n-2)} + (\frac{\ln \ln n - n}{n(\ln \ln n)^2}) + (P-N) \otimes (P+N) \end{cases} . \quad (35)$$

Вирішуючи систему диференціальних рівнянь (35) відносно параметру захисту соціальної мережі, визначимо коефіцієнт захисту соціальної мережі:

$$K_z = \frac{\sum_{i=1}^{n}(C_D{}'(i) - C_D(i))}{(n-1)(n-2)} + D_i + DR + (N(r+1)\wedge(-f)) - (\frac{\sum_{v\in V} C_{v1}}{n^2}) + \\ + (P-N)*(P+N) + (\alpha+\beta+\theta+\rho)V + \frac{\ln\ln n - n}{n(\ln\ln n)^2} \quad , \qquad (36)$$

де D_i – коефіцієнт, що відображає вплив загроз безпеки даних від втрати довіри між користувачами на захищеність інформаційної системи;

DR – коефіцієнт, що відображає вплив загроз безпеки даних від втрати репутації між користувачами на захищеність інформаційної системи; $N(r+1)\wedge(-f)$ – коефіцієнт, що відображає вплив загроз безпеки даних від розповсюдження інформації між користувачами на захищеність інформаційної системи;

$\frac{\sum_{v\in V} C_{v1}}{n^2}$ – коефіцієнт, що відображає вплив загроз безпеки даних від коефіцієнта кластеризації мережі на захищеність інформаційної системи; - $(P-N)\otimes(P+N)$ – коефіцієнт, що відображає вплив загроз безпеки даних від взаємовпливу користувачів на захищеність інформаційної системи; $(\alpha+\beta+\theta+\rho)V$ – коефіцієнт, що відображає вплив загроз безпеки даних від взаємодії користувачів на захищеність інформаційної системи;

$\frac{\ln\ln n - n}{n(\ln\ln n)^2}$ – коефіцієнт, що відображає вплив загроз безпеки даних від довжини шляху між користувачами на захищеність інформаційної системи.

Вираз (36) остаточно визначає математичну модель захисту інформації в соціальної мережі від специфічних параметрів. Таких як: довіра, репутація, вплив загроз безпеки даних від розповсюдження інформації між користувачами, вплив загроз безпеки даних від взаємовпливу користувачів, вплив загроз безпеки даних від взаємодії користувачів та вплив загроз безпеки даних від довжини шляху між користувачами. Слід означити , що параметрів соціальної мережи значно більше. Але ці параметри ми вважаємо найбільш впливові.

Використовуючи удосконалену модель, проведемо моделювання процесу захисту інформації в соціальної мережи з урахуванням специфічних параметрів соціальної мережи. При моделюванні використовували обмеження: усі коефіцієнти нормовані та не перевищують одиницю. Припущення усі специфічні параметри соціальної мережи підпорядковуються нормальному закону розповсюдження. З застосуванням цих припущень та обмежень проведемо моделювання. Результати моделювання наведемо в вигляди рисунку. Результати моделювання представлені у графічному вигляді на рис. 1.

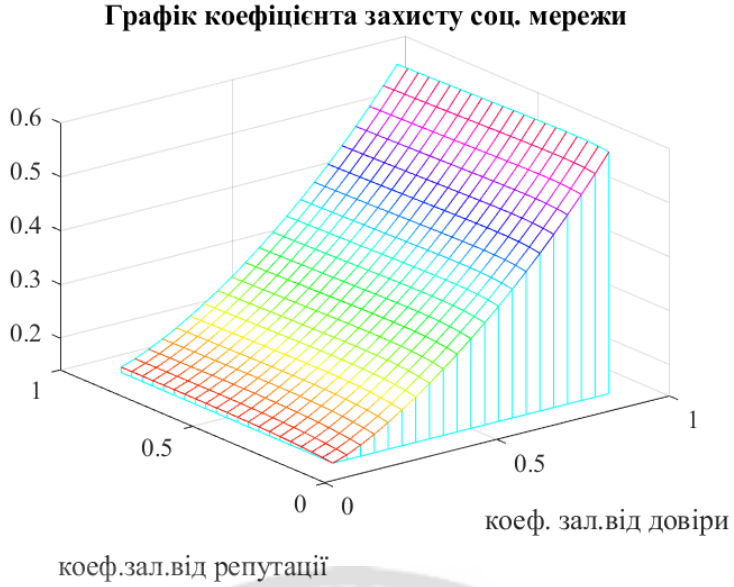

Рисунок 1 – Залежність коефіцієнта захисту соціальної мережі від коефіцієнтів пов'язаних з довірою та репутацією

Як бачимо з графіка коефіцієнт захисту соціальної мережи не приймає нулеві значення, що цілком відповідає реальності. Не може бути захист інформації при відсутності довіри до інформації, інформація у такому випадку просто існує та не потрібує захисту бо користувачу інформація не потрібна. Бачимо що коефіцієнті ,які залежать від репутації на багато менш впливають на коефіцієнт захисту ніж коефіцієнти. Які залежать від довіри. Це теж цілком відповідає сенсу, бо параметр репутації це необхідна умова, але не достатня. Достатній умовою е довіра.

Таким чином результати моделювання остаточно довели, що головним параметром який впливає на захист інформації є параметр довіри. Другі специфічні параметри соціальної мережи впливають на коефіцієнт захисту у значно менший мірі.

Висновки. Розроблено удосконалена математичної моделі захисту інформації в соціальної мережі в залежності від специфічних її параметрів. Таких як: довіра, репутація, вплив загроз безпеки даних від розповсюдження інформації між користувачами, вплив загроз безпеки даних від взаємовплив користувачів, вплив загроз безпеки даних від взаємодії користувачів та вплив загроз безпеки даних від довжини шляху між користувачами.

Проведено математичне моделювання удосконаленої моделі захисту інформації у соціальної мережі в залежності від специфічних її параметрів. Графічні результати відображають актуальну картину захисту інформації соціальної мережи від зовнішніх впливів. Отримані результати для узагальненого коефіцієнта захисту соціальної мережи, показують що коефіцієнт захисту не приймає нулеві значення, що цілком відповідає реальності. Не може бути захист інформації при відсутності довіри до інформації, інформація у такому випадку просто існує та не потрібує захисту бо користувачу інформація не потрібна. Результати моделювання показали, що коефіцієнті ,які залежать від репутації на багато менш впливають на коефіцієнт захисту ніж коефіцієнти, які залежать від довіри. Це доводить, що параметр репутації це необхідна умова, але не достатня. Достатній умовою е довіра. Отримані результати підтверджують адекватність розробленої математичної моделі захисту інформації у соціальної сеті

Подальший розвиток запропонованого методу полягає у більш детальному розгляді специфіки соціальної мережи та параметрів інформаційного захисту.

ЛІТЕРАТУРА:

1. Akhramovich V.M. Limit probabilities of data security and user interaction in the social network. Magyar Tudományos Journal. Budapest, Hungary. 2020. № 41. pp 25–31. www.magyar–journal.com.

2. Akhramovich V.M. Communication and influence of users in social networks. Colloquium–journal. Warszawa, Polska. 2020. №3 (55). pp. 21–25.

3. Oleg Barabash, Oleksandr Laptiev, Oksana Kovtun, Olga Leshchenko, Kseniia Dukhnovska, Anatoliy Biehun. The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 9, September 2020.pp 5713-5718. DOI:10.30534/ijeter/2020/130892020

4. Barabash Oleg, Laptiev Oleksandr, Tkachev Volodymyr, Maystrov Oleksii, Krasikov Oleksandr, Polovinkin Igor. The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 8, August 2020. Indexed- ISSN: 2278 – 3075. pp4133 – 4139. DOI:10.30534/ijeter/2020/17882020

5. Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksandr Laptiev, Svitlana Lehominova, Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.2019 – 2025. DOI:10.30534/ijeter/2020/90852020

6. Lubov Berkman, Oleg Barabash, Olga Tkachenko, Andri Musienko, Oleksandr Laptiev, Ivanna Salanda The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.1920 – 1925. DOI:10.30534/ijeter/2020/73852020

7. Laptiev Oleksandr, ShuklinGerman, Savchenko Vitalii, Barabash Oleg, MusienkoAndrii and Haidur Halyna, The Method of Hidden Transmitters Detection based on the Differential Transformation Model. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 8 No. 6 .November - December 2019. Scopus Indexed - ISSN 2278 – 3091.pp.2840 – 2846. DOI: 10.30534/ijatcse/2019/26862019

8. Olexandr Laptiev, German Shuklin, Spartak Hohonianc, Amina Zidan, Ivanna Salanda. Dynamic model of Ceber Defence Diagnostics of information Systems with the Use of Fozzy Technologies IEEE ATIT 2019 Conference Proceedings Kyiv, Ukraine, December 18-20, pp.116 –120.

9. Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Oleksandr Laptiev, Ivan Opirskyy, Olha No. 5, September-Oktober 2020, pp 8725-8729. DOI: 10.30534/ijatcse/2020/261952020 Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9.

10. Oleksandr Laptiev, Oleh Stefurak, Igor Polovinkin, Oleg Barabash, Savchenko Vitalii, Olena Zelikovska. The method of improving the signal detection quality by accounting for interference. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.172 –176.

11. Oleksandr Laptiev, Savchenko Vitalii, Serhii Yevseiev, Halyna Haidur, Sergii Gakhov, Spartak Hohoniants. The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.176 –181.

12. Valentyn Sobchuk, Volodymyr Pichkur, Oleg Barabash, Oleksandr Laptiev, Kovalchuk Igor, Amina Zidan. Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.206 –211.

13. Vitalii Savchenko, Oleksandr Laptiev, Oleksandr Kolos, Rostyslav Lisnevskyi, Viktoriia Ivannikova, Ivan Ablazov. Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.246 –251

14. Oleg Barabash, Andrii Musienko, Spartak Hohoniants, Oleksandr Laptiev, Oleg Salash, Yevgen Rudenko, Alla Klochko. Comprehensive Methods of Evaluation of Efficiency of Distance Learning System Functioning. International Journal of Computer Network and Information Security(IJCNIS), IJCNIS Vol. 13, No. 1, Feb. 2021. pp 16–28. DOI: 10.5815/ijcnis.2021.01.02

15. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615

16. Laptiev O., Savchenko V., Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., Biehun A. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.15-21.

17. Oleksandr Laptiev, Vitalii Savchenko, Andrii Pravdyvyi, Ivan Ablazov, Rostyslav Lisnevskyi, Oleksandr Kolos, Viktor Hudyma. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.48-54.

18. O. Svynchuk, O. Barabash, J. Nikodem, R. Kochan, O. Laptiev. Image compression using fractal functions.Fractal and Fractional, 2021, 5(2), 31.pp.1-14. DOI:10.3390/fractalfract5020031 - 14 Apr 2021

19. Oleg Barabash, Oleksandr Laptiev, Valentyn Sobchuk, Ivanna Salanda, Yulia Melnychuk, Valerii Lishchyna. Comprehensive Methods of Evaluation of Distance Learning System Functioning. International Journal of Computer Network and Information Security (IJCNIS). Vol. 13, No. 3, Jun. 2021. pp.62-71, DOI: 10.5815/ijcnis.2021.03.06

20. Bataeva I.P. Information protection and information security. NiKa. 2012№. URL: https://cyberleninka.ru/article/n/zaschita-informatsii-i-informatsionnaya (10.06.2019).

21. Пампуха І.В., Самолов І.В., Толюпа С.В., Берназ Н.М. Інтелектуальний підхід до управління мережними відмовами систем передачі даних. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К: ВІКНУ, 2008. № 20. С. 18 – 21.

22. A.O. Korchenko, V.O. Breslavskyi, S.P Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2021.225346

REFERENCES:

1. Akhramovich V.M. Limit probabilities of data security and user interaction in the social network. Magyar Tudományos Journal. Budapest, Hungary. 2020. № 41. pp 25–31. www.magyar–journal.com.

2. Akhramovich V.M. Communication and influence of users in social networks. Colloquium–journal. Warszawa, Polska. 2020. №3 (55). pp. 21–25.

3. Oleg Barabash, Oleksandr Laptiev, Oksana Kovtun, Olga Leshchenko, Kseniia Dukhnovska, Anatoliy Biehun. The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 9, September 2020.pp 5713-5718. DOI:10.30534/ijeter/2020/130892020

4. Barabash Oleg, Laptiev Oleksandr, Tkachev Volodymyr, Maystrov Oleksii, Krasikov Oleksandr, Polovinkin Igor. The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 8, August 2020. Indexed- ISSN: 2278 – 3075. pp4133 – 4139. DOI:10.30534/ijeter/2020/17882020

5. Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksandr Laptiev, Svitlana Lehominova, Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.2019 – 2025. DOI:10.30534/ijeter/2020/90852020

6. Lubov Berkman, Oleg Barabash, Olga Tkachenko , Andri Musienko, Oleksandr Laptiev, Ivanna Salanda The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.1920 – 1925. DOI:10.30534/ijeter/2020/73852020

7. Laptiev Oleksandr, ShuklinGerman, Savchenko Vitalii, Barabash Oleg, MusienkoAndrii and Haidur Halyna, The Method of Hidden Transmitters Detection based on the Differential Transformation Model. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 8 No. 6 .November - December 2019. Scopus Indexed - ISSN 2278 – 3091.pp.2840 – 2846. DOI: 10.30534/ijatcse/2019/26862019

8. Olexandr Laptiev, German Shuklin, Spartak Hohonianc, Amina Zidan, Ivanna Salanda. Dynamic model of Ceber Defence Diagnostics of information Systems with the Use of Fozzy Technologies IEEE ATIT 2019 Conference Proceedings Kyiv, Ukraine, December 18-20, pp.116 –120.

9.Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Oleksandr Laptiev, Ivan Opirskyy, Olha Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9. No. 5, September-Oktober 2020, pp 8725-8729. DOI: 10.30534/ijatcse/2020/261952020

10. Oleksandr Laptiev, Oleh Stefurak, Igor Polovinkin, Oleg Barabash, Savchenko Vitalii, Olena Zelikovska. The method of improving the signal detection quality by accounting for interference. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.172 –176.

11. Oleksandr Laptiev, Savchenko Vitalii, Serhii Yevseiev, Halyna Haidur, Sergii Gakhov, Spartak Hohoniants. The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.176 –181.

12. Valentyn Sobchuk, Volodymyr Pichkur, Oleg Barabash, Oleksandr Laptiev, Kovalchuk Igor, Amina Zidan. Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.206 –211.

13. Vitalii Savchenko, Oleksandr Laptiev, Oleksandr Kolos, Rostyslav Lisnevskyi, Viktoriia Ivannikova, Ivan Ablazov. Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.246 –251

14. Oleg Barabash, Andrii Musienko, Spartak Hohoniants, Oleksandr Laptiev, Oleg Salash, Yevgen Rudenko, Alla Klochko. Comprehensive Methods of Evaluation of Efficiency of Distance Learning System Functioning. International Journal of Computer Network and Information Security(IJCNIS), IJCNIS Vol. 13, No. 1, Feb. 2021. pp 16–28. DOI: 10.5815/ijcnis.2021.01.02

15. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615

16. Laptiev O., Savchenko V., Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., Biehun A. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.15-21.

17. Oleksandr Laptiev, Vitalii Savchenko, Andrii Pravdyvyi, Ivan Ablazov, Rostyslav Lisnevskyi, Oleksandr Kolos, Viktor Hudyma. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.48-54.

18. O.Svynchuk, O. Barabash, J.Nikodem, R. Kochan, O. Laptiev. Image compression using fractal functions.Fractal and Fractional, 2021, 5(2), 31.pp.1-14. DOI:10.3390/fractalfract5020031 - 14 Apr 2021

19. Oleg Barabash, Oleksandr Laptiev, Valentyn Sobchuk, Ivanna Salanda, Yulia Melnychuk, Valerii Lishchyna. Comprehensive Methods of Evaluation of Distance Learning System Functioning. International Journal of Computer Network and Information Security (IJCNIS). Vol. 13, No. 3, Jun. 2021. pp.62-71, DOI: 10.5815/ijcnis.2021.03.06

20. Bataeva I.P. Information protection and information security. NiKa. 2012№. URL: https://cyberleninka.ru/article/n/zaschita-informatsii-i-informatsionnaya (10.06.2019).

21. Pampukha I.V., Samolov I.V., Toliupa S.V., Bernaz N.M. (2008), "Intelektualnyi pidkhid do upravlinnia merezhnymy vidmovamy system peredachi danykh" [An intelligent approach to network failure management of data transmission systems]. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Kyiv: VIKNU, 2008. No. 20. P. 18 – 21.

22. A.O. Korchenko, V.O. Breslavskyi, S.P Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2021.225346

D.Sci.Tech. Lukova-Chuiko N.V., D.Sci.Tech. Toliupa S.V., Phd Pogasiy S.S., Laptieva T.O., Laptiev S.O.

IMPROVEMENT OF THE MODEL OF INFORMATION PROTECTION IN SOCIAL NETWORKS

In Ukraine, the right to privacy is a constitutional guarantee, and the protection of personal data is one of the areas in which such a guarantee should be implemented. The subject of our research will not be objects in general, but dynamic systems of information protection in social networks in the mathematical sense of the term. Descriptions of dynamical systems for various problems depending on the law of evolution are various: by means of differential equations, discrete mappings, the theory of graphs, the theory of Markov chains, etc. The choice of one of the methods of description determines the specific form of the mathematical model of the corresponding dynamic system. Theoretical study of the dynamic behavior of a real object requires the creation of its mathematical model. Most of the known approaches to modeling differ in what parameters they use as input information in modeling and what characteristics of the simulated system are calculated and output to the model. The article presents the development of an improved mathematical model of information protection in a social network depending on its specific parameters. Such as trust, reputation, the impact of data security threats from the dissemination of information between users, the impact of data security threats from user interactions, the impact of data security threats from user interaction, and the impact of data security threats from the length of the path between users. However, it should be noted that the parameters of the social network are much more. But we consider these parameters to be the most influential. Therefore, we pay attention to these specific parameters.

Mathematical modeling of the improved model of information protection in the social network depending on its specific parameters is carried out. Graphic results reflect the current picture of protection of social network information from external influences. The obtained results confirm the adequacy of the developed mathematical model of information protection in the social network.

Keywords: social network, trust, reputation, modeling, protection factor, security, information protection.